



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/499,736	02/08/2000	Pierre Calvez	T2147-906343	1674
7590	04/05/2005		EXAMINER	
Miles & Stockbridge PC. 1751 Pinnacle Drive Suite 500 McLean, VA 22102-3833			SIMITOSKI, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/499,736	CALVEZ ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) Responsive to communication(s) filed on 14 January 2005.
- 2a) This action is **FINAL**.                            2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) Claim(s) 15-35 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) 29 and 30 is/are allowed.
- 6) Claim(s) 15-28 and 31-35 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 14 January 2005 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All    b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_.
- 4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. The response of 1/14/2005 was received and considered.
2. Claims 15-35 are pending.
3. Claims 29 & 30 are allowed.
4. The drawings submitted with Applicant's are substantively acceptable, however, the submission fails to comply with 37 CFR §1.121(d), which requires that submitted drawing sheets must be labeled "Replacement Sheet". Corrected drawings are required. The requirement for corrected drawings will not be held in abeyance.

#### ***Response to Arguments***

5. In light of Applicant's response, the objections to claims 22 & 24-26, set forth in the previous Office Action, are withdrawn.
6. Applicant's arguments filed 1/14/2005 have been fully considered but they are not persuasive.
7. Applicant's response cites two portions of Euchner (col. 2, lines 33-39 & col. 3, lines 5-11) stating that

"neither this portion nor any other portion of Euchner teaches or suggests that the challenge includes information representing whether a network authentication has been performed" and

"as stated in the Abstract of Euchner, authentication references that are employed in further cryptographic phrases are exchanged during authentication of the first computer unit and a second computer unit".

Art Unit: 2134

8. However, neither of these sections are relied upon by the Examiner. Applicant has provided no argument as to why the reference fails to apply read on the claims, but rather to cite portions of the reference and generally suggest that the rejection is misplaced. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. From the cited portions, it appears that Applicant is relying on the cited portions of Euchner to imply that only one authentication is performed. The claim language of the instant invention recites "the type of challenge representing whether a network authentication has been performed". The Euchner reference teaches a well-known concept in cryptography, where protocol instances are distinguished using increasing values (col. 6, line 66 – col. 7, line 6). This prevents replay attacks, as stated in Euchner (col. 6, line 66 – col. 7, line 6). It is noted that the claim language of the instant invention, and specifically the type of challenge, does not require the network authentication to have been performed twice on the same device. Further, the type of challenge which indicates whether network authentication has been performed does not require a *successful* authentication, but simply that an authentication has been performed. In this light, the Euchner reference is cited for teaching that multiple instances of an authentication protocol contain a count value, making each instance unique. By receiving later protocol instances with either a higher count than a previous instance, or of a count greater than an initial count, the receiver of the challenge knows that authentication has been previously performed.

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 15-23, 27-28 & 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over the SKID protocol, described in Applied Cryptography, Second Edition, by Bruce Schneier, published 1996, in view of U.S. Patent 6,014,085 to Patel, in further view of U.S. Patent 6,401,204 to Euchner et al. (Euchner).

Regarding claims 15, 27 & 28, Schneier discloses Alice being a user/local machine and Bob being a host/server (p. 52, ¶1 and p. 55, ¶1). Schneier discloses creating a challenge/random number and communicating it along with elements known by the user/“A” to the server/“B” (p. 55, step 1 and p. 56, step 3). Schneier discloses performing a calculation/hash, obtaining a first response/ $R_B, H_k(R_A, R_B, B)$  and transmitting that response (p. 55, step 2) to the user/“A” by the server/“B”/administrator. Schneier discloses performing a second calculation/hash that is a function of predetermined data and comparing the results (p. 56, step 3). Schneier lacks the challenge including information representing the type of challenge. However, Patel teaches that to avoid replay attacks in an authentication system, it is beneficial to use challenge codes representing different challenge types to determine authentication codes (col. 5, lines 5-36) and that one type of challenge code is a version number (col. 6, lines 39-66). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a version number and information indicating the type of challenge. One of ordinary skill

in the art would have been motivated to perform such a modification to prevent impersonators from successfully realizing replay attacks, as taught by Patel (col. 5, lines 5-36 & col. 6, lines 39-66). As modified, Schneier lacks the challenge type indicating whether a network authentication has been performed. However, Euchner teaches that in an authentication protocol (col. 2, lines 26-33), a count value is included in the messages to distinguish between different protocol runs for the same connection (col. 6, line 66 – col. 7, line 6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to indicate whether a network authentication has been performed. One of ordinary skill in the art would have been motivated to perform such a modification to distinguish between different protocol runs, as taught by Euchner (col. 2, lines 26-33 & col. 6, line 66 – col. 7, line 6).

Regarding claims 16-18, Schneier discloses a hash being performed over the challenge/random number and at least one secret/k (p. 55, step 2 and p. 55, step 3).

Regarding claims 19-21, Schneier, as modified above, lacks the act of sharing a secret value. However, Schneier teaches that “In general, a man-in-the-middle attack can defeat any protocol that doesn’t involve a secret of some kind.” Schneier further teaches that protocols that combine authentication with key exchange solve a general computer problem wherein different users want to communicate securely (p. 56, 2<sup>nd</sup> paragraph). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish a secret key between the local machine and server to enable secure communication after authentication. One of ordinary skill in the art would have been motivated to perform such a modification to enable secure communication and to secure the transaction from the man-in-the-middle attack, as taught by Schneier.

Regarding claim 22, Schneier, as modified above, lacks modifying a shared secret with a key that depends on the local machine. However, in a discussion of key-exchange protocols, Schneier discloses that public key cryptography makes key exchange easier, in that a first party encrypts a secret with the public key of a second party. This allows only the second party access to the secret (p. 48). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the shared secret with a key that depends on the local machine to make key exchange easier. One of ordinary skill in the art would have been motivated to perform such a modification to make key exchange easier, as taught by Schneier (p. 48).

Regarding claim 23, Schneier discloses a byte string consisting of hashing a Master Station Secret/R<sub>A</sub> to obtain a Station Secret/H<sub>k</sub>(R<sub>A</sub>,R<sub>B</sub>,B) (p. 55, step 2).

Regarding claim 31, Schneier discloses a response/H<sub>k</sub>(R<sub>A</sub>,R<sub>B</sub>,B) composed of hashing a string composed of a user's password/K, a Station Secret/R<sub>A</sub> and the user name/B (p. 55, step 2).

Regarding claim 32, Schneier discloses a response/H<sub>k</sub>(R<sub>A</sub>,R<sub>B</sub>,B) composed of hashing a string composed of a fixed security key/K stored in the local machine/B and server/A, the name of the local machine/B (p. 55, step 2).

11. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,161,185 to Guthrie et al. (Guthrie) in view of Patel in further view of Euchner. Guthrie discloses a user (Fig. 5, element 114), local machine (Fig. 5, element 102) and remote server (Fig. 5, element 104), means for classifying information (Fig. 5, element 120) and communication means (Fig. 5, element 112 & 118). Guthrie further discloses a system

administrator (col. 2, lines 42-47), a local machine comprising an authentication module that include a first user module (Fig. 5, element 126) for generating a challenge (Fig. 4, element 114) and second user module for generating a response (Fig. 5, element 130) and an administrative authentication module for authorizing access (Fig. 5, element 132). Guthrie lacks the challenge including information representing the type of challenge. However, Patel teaches that to avoid replay attacks in an authentication system, it is beneficial to use challenge codes representing different challenge types to determine authentication codes (col. 5, lines 5-36) and that one type of challenge code is a version number (col. 6, lines 39-66). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a version number and information indicating the type of challenge. One of ordinary skill in the art would have been motivated to perform such a modification to prevent impersonators from successfully realizing replay attacks (col. 5, lines 5-36 & col. 6, lines 39-66). As modified, Guthrie lacks the challenge type indicating whether a network authentication has been performed. However, Euchner teaches that in an authentication protocol (col. 2, lines 26-33), a count value is included in the messages to distinguish between different protocol runs for the same connection (col. 6, line 66 – col. 7, line 6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to indicate whether a network authentication has been performed. One of ordinary skill in the art would have been motivated to perform such a modification to distinguish between different protocol runs, as taught by Euchner (col. 2, lines 26-33 & col. 6, line 66 – col. 7, line 6).

Art Unit: 2134

12. Claims 24, 25 & 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Patel & Euchner, as applied to claims 16, 17 & 18 above, in further view of U.S. Patent 5,081,677 to Green et al. (Green). Schneier, as modified above, lacks a version number associated with a shared secret, and incremented when the shared secret is modified. However, Green teaches that, when updating a master key, it is useful to associate a version number with a the key and to increment the version number when the key is modified, to enable distributed copies of the key to be updated on first use and to modify the master key without exposing it to applications (col. 2, lines 30-67 & col. 3, lines 5-35). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to associate a version number with a shared secret and to increment the version number when the secret is modified. One of ordinary skill in the art would have been motivated to perform such a modification to enable the shared secrets to be updated at different times (on first use) and to enable modification of the secret without exposing it, as taught by Green (col. 2, lines 30-67 & col. 3, lines 5-35).

13. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Patel & Euchner, as applied to claim 15 above, in view of U.S. Patent 5,774,650 to Chapman et al. (Chapman). Schneier, as modified above, lacks temporary authorization where the duration is configurable. However, Chapman teaches time-limited access to a system is beneficial to temporarily enable a privileged user to use the full performance capability of a system by temporarily denying access to less-privileged users (col. 2, lines 38-61). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a time-based authorization in Schneier's system to enable a privileged user to access the

Art Unit: 2134

full capabilities of the system. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of enabling a user to temporarily gain full access to a system's resources, as taught by Chapman (col. 2, lines 38-61).

14. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Patel & Euchner, as applied to claim 15 above, in view of Windows NT User Administration, by Ashley J. Meggitt & Timothy D. Ritchey (Meggitt). Schneier, as modified above, lacks specific disclosure of locally authenticating a user after disconnection. However, Meggitt teaches that Windows NT allows a user, normally authenticated through a domain, to login to a local workstation even if the roaming profile is unavailable (p. 139). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the authentication protocol taught by Schneier to allow login to a local machine by a user, usually authenticated remotely, in the case that network connectivity has been disrupted. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of local system access even when remote authentication is unavailable, as taught by Meggitt (p. 139).

***Allowable Subject Matter***

15. Claims 29 & 30 are allowed.

16. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 29 & 30, the prior art relied upon fails to specifically teach the limitation of a challenge composed of a first byte representing the type of challenge, the type of challenge indicating whether a network authentication has been performed; second and third

Art Unit: 2134

bytes representing the version number of the shared information; and random alphanumeric characters of the fourth to twelfth bytes.

***Conclusion***

17. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks  
Washington, DC 20231

**Or faxed to:**

Art Unit: 2134

(703)746-7239 (for formal communications intended for entry)

Or:

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJS

March 23, 2005



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100